

SMART AI SYSTEM FOR MALICIOUS URL AND CYBER THREAT DETECTION

Dr.Madhubala^{P1}, Harini P², Kanushya E³, Karthiga G⁴,Arthi M⁵

¹Associate Professor, Computer Science and Engineering, Bharathiyar Institute of Engineering
For Women (Autonomous)

^{2,3,4,5} UG Student, Computer Science and Engineering, Bharathiyar Institute of Engineering
For Women (Autonomous)

Abstract-With the rapid expansion of internet technologies and online services, cybersecurity threats have become a major concern for individuals, organizations, and governments. Among these threats, malicious URLs play a significant role in cyber-attacks such as phishing, malware distribution, identity theft, and financial fraud. Attackers frequently create deceptive web links that appear legitimate to trick users into revealing sensitive information or downloading harmful software. Traditional security systems, including blacklist-based detection methods, often fail to identify newly generated or dynamically changing malicious URLs. This research proposes is designed to identify and prevent harmful online activities in real time. The proposed system integrates advanced machine learning techniques with intelligent data analysis to detect suspicious URLs based on multiple characteristics such as lexical features, domain information, URL length, special characters, host-based attributes, and behavioural patterns. The SMART AI framework includes several stages such as data collection, data preprocessing, feature extraction, model training, and real-time threat classification.

Keywords: Cyber security Threats, Malicious URLs, Financial Fraud

1.Introduction

The rapid development of internet technologies and the increasing dependence on digital platforms have significantly transformed the way individuals and organizations communicate, conduct business, and access information. Online services such as e-commerce, online banking, cloud computing, and social networking have become essential parts of modern life. However, this rapid digital transformation has also created new opportunities for cybercriminals to exploit vulnerabilities in online systems. As a result, cybersecurity has become a critical concern for governments, industries, and individuals worldwide.

One of the most common methods used by cyber attackers is the use of malicious URLs. A malicious URL is a web link designed to direct users to harmful websites that may steal sensitive information, install malware, or perform

unauthorized activities on the user's device. These URLs are frequently used in phishing emails, fake advertisements, and social media messages to trick users into clicking them. Once the user interacts with such links, attackers can gain access to confidential information such as passwords, banking details, and personal data. Due to the increasing number of online users, the number of malicious URLs and cyber threats is also growing rapidly.

Traditional security systems rely mainly on blacklist-based techniques or signature-based detection methods to identify malicious links. Although these approaches can detect previously known threats, they often fail to recognize newly generated or modified malicious URLs. Cyber attackers continuously change the structure and appearance of URLs to bypass traditional security mechanisms. Therefore, conventional detection techniques are not sufficient to handle the dynamic and evolving nature of modern cyber threats.

To address these challenges, researchers and cybersecurity experts are increasingly exploring the use of Artificial Intelligence (AI) and Machine Learning (ML) techniques for threat detection. AI-based systems have the ability to analyze large volumes of data, identify hidden patterns, and detect anomalies that may indicate malicious behavior. By learning from historical data and continuously adapting to new attack patterns, AI models can provide more accurate and efficient cyber threat detection compared to traditional methods.

This research proposes a SMART AI system for malicious URL and cyber threat detection, which integrates intelligent data analysis and machine learning algorithms to identify harmful URLs and suspicious online activities. The proposed system focuses on extracting important features from URLs, such as lexical characteristics, domain-related attributes, and behavioral patterns. These features are then analyzed using machine learning models to classify URLs as either legitimate or malicious. The SMART AI framework aims to improve detection accuracy, reduce false positives, and provide real-time threat identification.

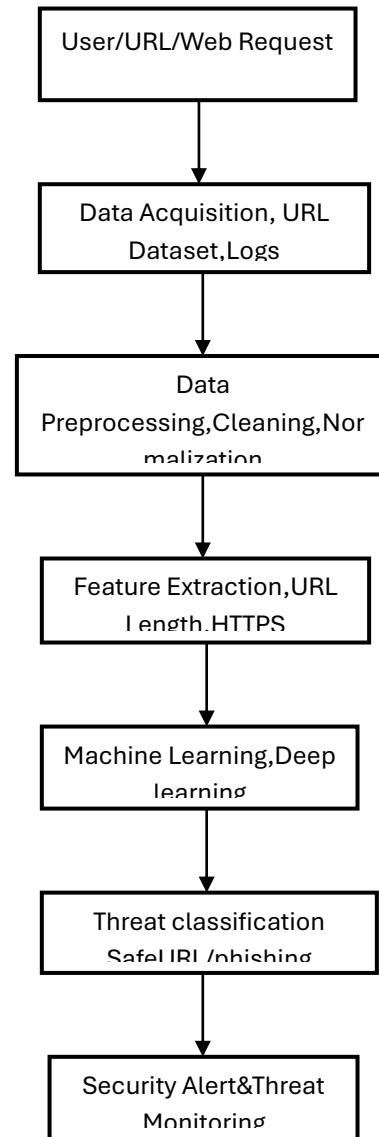
Furthermore, the proposed system is designed to adapt to emerging cyber threats by continuously learning from new datasets and updating its detection models. This capability enables the system to identify previously unseen malicious URLs and protect users from sophisticated cyber-attacks. Malicious URLs. As cyber attackers continuously generate new URLs and modify existing patterns, researchers have focused on developing intelligent detection systems using Artificial Intelligence (AI) and Machine Learning (ML).

Machine learning-based detection systems analyze large datasets of both malicious and legitimate URLs to identify patterns and classify them accurately. These systems extract various features from URLs, such as lexical features (URL length, number of special characters, number of subdomains), host-based features (domain age, DNS information, IP address), and content-based features (HTML scripts and webpage content). Using these features, machine learning algorithms such as Random Forest, Support Vector Machine (SVM), Decision Tree, and Logistic Regression are trained to detect suspicious URLs. Studies have shown that these algorithms can significantly improve detection accuracy compared to traditional methods and can identify previously unseen threats.

In recent years, deep learning techniques have been introduced to further enhance malicious URL detection systems. Models such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) networks are capable of automatically learning complex patterns directly from raw URL strings without the need for manual feature extraction. These deep learning models can process large-scale datasets and detect sophisticated cyber threats with higher accuracy. Many research works have demonstrated that combining deep learning models with feature-based approaches improves detection performance and reduces false positives.

Despite these advancements, several challenges remain in malicious URL detection. Attackers frequently change URL structures to evade detection, and the large volume of web traffic makes real-time analysis difficult. Additionally, many datasets used for training are imbalanced, which can affect model performance. Researchers are therefore exploring hybrid AI systems that integrate machine learning, deep learning, and threat intelligence data to improve detection capability. Overall, the literature indicates that smart AI-based systems play a crucial role in identifying malicious URLs and preventing cyber threats, and future research is expected to focus on more adaptive, scalable, and real-time detection mechanisms.

2. DIAGRAM



3. METHODOLOGY

The proposed Smart AI System for Malicious URL and Cyber Threat Detection is designed to automatically identify and classify suspicious URLs using artificial intelligence and machine learning techniques. The methodology consists of several stages, including data collection, preprocessing, feature extraction, model training, threat detection, and system evaluation.

In the first stage, data collection, a large dataset of URLs is gathered from publicly available cybersecurity repositories, phishing databases, and network traffic logs. The dataset contains both malicious and legitimate URLs to ensure that the model can learn to differentiate between harmful and safe websites. These datasets may include phishing URLs, malware distribution links, and normal web addresses.

The second stage involves data preprocessing, where the collected data is cleaned and prepared for analysis. This

step includes removing duplicate URLs, handling missing values, normalizing data formats, and labeling URLs as either malicious or benign. Preprocessing helps improve the quality of the dataset and ensures accurate model training.

The next stage is feature extraction, which is one of the most important steps in malicious URL detection. In this step, different characteristics of the URLs are analyzed to create meaningful features for the machine learning model. These features include lexical features such as URL length, number of special characters, presence of IP addresses, number of subdomains, and suspicious keywords. Host-based features such as domain age, DNS records, and HTTPS usage may also be extracted to provide additional information about the website.

After feature extraction, the dataset is divided into training and testing sets. The training data is used to build and train the machine learning model, while the testing data is used to evaluate the model's performance. Various machine learning algorithms such as Random Forest, Support Vector Machine (SVM), Decision Tree, or Logistic Regression can be used to classify URLs as malicious or legitimate. The model learns patterns from the training data and builds a predictive model for detecting cyber threats.

3.1 Data Collection: As part of an ongoing research project, we collected 93 cyberattacks along with three descriptions explaining the attack compiled from publicly available security blogs and threat repositories such as: CWE [16], CAPEC [17] and ATT&CK [18]. We then annotated these attacks with 50 non-technical consequence descriptions, which are written in simple language (i.e., layman terms) so they can be understood by security practitioners as well as CPS end-users. This is important for communication because various stakeholders who make decisions about cyberattack mitigation and strategy plans have little to no security knowledge. The 50 consequences were then grouped into 7 clusters based on the similarity between the consequences. The process involved an open card sort activity through which were recruited a number of participants to sort and group the 50 consequences into groups. shows some of the attacks, consequences and their cluster number. The cluster numbers and their labels are described. We only list the cluster labels and not the 50 individual consequences for brevity.

3.2 Text Cleaning: The text data in the attack descriptions needs to be preprocessed before it can be useful for further processing. Text cleaning or pre-processing involves removing stop words (such as articles), punctuation, digits, stemming and lemmatization. We used clean-text library1 to convert the text into lower case and remove stopwords and punctuation. After this step, the text descriptions can be used for feature extraction.

4.CONCLUSION

In conclusion, the development of a Smart AI System for Malicious URL and Cyber Threat Detection plays a significant role in enhancing cybersecurity and protecting users from online threats. Malicious URLs are widely used in phishing attacks, malware distribution, and other cyber crimes, making it essential to detect and prevent them effectively. Traditional detection methods such as blacklist and signature-based techniques are limited in their ability to identify newly created or unknown malicious URLs.

The use of Artificial Intelligence and Machine Learning techniques provides a more advanced and efficient solution for detecting cyber threats. By analyzing various features of URLs and learning patterns from large datasets, AI-based systems can accurately classify URLs as malicious or legitimate. Machine learning algorithms such as

Random Forest, Support Vector Machine, and Decision Tree improve detection accuracy and help identify previously unseen threats.

5.REFERENCE

- [1] N. I. of Standard Technology. Cyber-physical systems. <https://www.nist.gov/el/cyber-physical-systems>.
- [2] S. Walker-Roberts, M. Hammoudeh, O. Aldabbas, M. Aydin, and A. Dehghantanha, "Threats on the horizon: Understanding security threats in the era of cyber-physical systems," *The Journal of Supercomputing*, vol. 76, no. 4, pp. 2643–2664, 2020.
- [3] M. N. Al-Mhiqani, R. Ahmad, W. Yassin, A. Hassan, Z. Z. Abidin, N. S. Ali, and K. H. Abdulkareem, "Cyber-security incidents: A review cases in cyber-physical systems," *International Journal of Advanced Computer Science and Applications*, vol. 9, 2018.
- [4] D. Serpanos, "The cyber-physical systems revolution," *Computer*, vol. 51, no. 3, pp. 70–73, 2018.
- [5] J.-P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocessors and Microsystems*, vol. 77, p. 103201, 2020. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0141933120303689>
- [6] M. R. Endsley, "Design and evaluation for situation awareness enhancement," *Proceedings of the Human Factors Society Annual Meeting*, vol. 32, no. 2, pp. 97–101, 1988.
- [7] R. S. Gutzwiller, S. M. Hunt, and D. S. Lange, "A task analysis toward characterizing cyber-cognitive situation

awareness (ccsa) in cyber defense analysts,” in 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2016, pp. 14–20.

[8] T. Debatty and W. Mees, “Building a cyber range for training cyberdefense situation awareness,” in 2019 International Conference on Military Communications and Information Systems (ICMCIS), 2019, pp. 1–6.

[9] J. Preden, “Generating situation awareness in cyber-physical systems: Creation and exchange of situational information,” in 2014 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), 2014, pp. 1–3.

[10] Z. Yang, T. Li, and W. Jiang, “Situation awareness for cyber-physical system: A case study of advanced metering infrastructure,” in 2018 IEEE International Conference on Prognostics and Health Management (ICPHM), 2018, pp. 1–6.

[11] H. Orojloo and M. Abdollahi Azgomi, “Predicting the behavior of attackers and the consequences of attacks against cyber-physical systems,” *Security and Communication Networks*, vol. 9, no. 18, pp. 6111–6136, 2016. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1761>

[12] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, “Challenges for securing cyber physical systems,” in *Workshop on Future Directions in Cyber-physical Systems Security*. DHS, July 2009.

[13] C. D. Manning, H. Schutze, and P. Raghavan, “Introduction to information retrieval. Cambridge university press, 2008.

[14] Q. V. Le and T. Mikolov, “Distributed representations of sentences and documents,” *CoRR*, vol. abs/1405.4053, 2014. Mikolov, I. Sutskever, K. Chen, G. S. Corrado, and J. Dean, “Distributed representations of words and phrases and their compositionality,” in *Advances in Neural Information Processing Systems*, C. J. C. Burges, L. Bottou, M. Welling, Z. Ghahramani, and K. Q. Weinberger, Eds., vol. 26. Curran Associates, Inc., 2013, pp. 3111–3119. 2013/file/9aa42b31882ec039965f3c4923ce901b-Paper.pdf

[15] MITRE. Cwe - common weakness enumeration.

[16] . Capec - common attack pattern enumeration and classification.

[17] . Mitre att&ck

[18] OWASP. Log injection software attack. [Online]. Available: <https://owasp.org/www-community/attacks/LogInjection>

[19] P. University. Secure internet programming: Web spoofing.

[20] Kaspersky. What is dns cache poisoning and dns spoofing? [Online]. Available: <https://usa.kaspersky.com/resource-center/definitions/dns>